



**National Student Clearinghouse®**  
2300 Dulles Station Boulevard, Suite 300  
Herndon, Virginia 20171

703-742-4200  
[www.studentclearinghouse.org](http://www.studentclearinghouse.org)

© 2009 National Student Clearinghouse. All rights reserved.

---

## File Encryption

The Clearinghouse provides [Secure File Transfer Protocol](#) (FTP) for the secure exchange of data files. With Secure FTP, passwords and files are automatically encrypted for transmission, with no user involvement, no key management and no need for additional encryption such as PGP. Built-in cryptography automatically encrypts the data as the file is being transferred, and re-encrypts the file prior to its being written to disk on the Secure FTP server. At no point is the file ever available "in the clear," even after transmission is complete. Users can be assured that their data is safe without further encryption with PGP. However, the Clearinghouse continues to support PGP encryption in cases where clients wish (or are required) to further encrypt their files with PGP.

PGP utilizes public key cryptography to encrypt files. Public key cryptography is an encryption scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a private key for decryption. You publish your public key to all trading partners while keeping your private key secret. To send encrypted data to the Clearinghouse, you must obtain the Clearinghouse's public key and encrypt the file with that key. In order for you to receive encrypted data from the Clearinghouse, the Clearinghouse must obtain your public key and encrypt the file with your key. Public keys are distributed in a physical file that can be emailed or downloaded via the Web.

### How to Encrypt Your Files

Follow these steps to use PGP to encrypt your files:

1. Download and install PGP from <http://www.pgpi.org/>
2. Download the Clearinghouse's public key (see instructions below)
3. Import the Clearinghouse's public key into your keyring

You are now ready to begin encrypting your data files, following these guidelines:

- Recent versions of PGP support DSS/Diffie-Hellman keys, which are preferred over RSA keys. The Clearinghouse supports both.
- For the highest level of security, choose key sizes of at least 1024 bits for encryption and digital signatures
- Electronically signing your files is not necessary, but provides a higher level of security.
- Compression is built into the encryption algorithm, so you don't need to zip your data files before or after encryption.

### How to Receive Encrypted Files

Follow these steps to receive encrypted files:

1. Download and install PGP from <http://www.pgpi.org/>
2. Generate public/private keys
3. Provide the Clearinghouse with your public key

### Download the Clearinghouse's Public Keys

- DSS/Diffie-Hellman key (for PGP v5.0 and above). Download from:  
[https://www.studentclearinghouse.org/secure\\_area/pgp/ClearinghousePublicKey.asc](https://www.studentclearinghouse.org/secure_area/pgp/ClearinghousePublicKey.asc)
- RSA key (for PGP v2.6 and above). Download from:  
[https://www.studentclearinghouse.org/secure\\_area/pgp/ClearinghousePublicKeyRSA.asc](https://www.studentclearinghouse.org/secure_area/pgp/ClearinghousePublicKeyRSA.asc)